

09/344,693

## BEST AVAILABLE COPY

### REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

### I. REJECTION OF CLAIMS 1-3, 18-20 AND 35-37 UNDER 35 U.S.C. § 102

Claims 1-3, 18-20 and 35-37 stand rejected as being anticipated by the Bots et al. patent (United States Patent No. 6,226,748, issued May 1, 2001, hereinafter "Bots"). The Applicants respectfully traverse the rejection.

Bots teaches a virtual private network (VPN) unit that serves as an endpoint of a VPN and moderates data communications between members of the VPN. Specifically, each site (e.g., a company headquarters, a company branch, a client site, etc.) in a VPN is associated with a VPN unit that implements a combination of techniques (e.g., compression, encryption, etc.) defined for data packet handling when packets are sent between members of the VPN. For example, a first VPN member at company headquarters may wish to send a secure communication to a second VPN member at a branch office. The VPN unit associated with the company headquarters will examine the (at this point, unencrypted) communication, determine that the destination is another VPN member, and compress, encrypt or authenticate the communication as required by policies for the VPN. A VPN unit associated with the branch office will treat the communication in a similar manner before delivering the communication, unencrypted, to the second user.

The Examiner's attention is directed to the fact that Bots fails to disclose or suggest the novel invention of a virtual private network in which a master node controls the admission and departure of a subset of member nodes, where all communications between the member nodes are encrypted, as claimed in Applicants' independent claims 1, 18 and 35. Specifically, Applicants' claims 1, 18 and 35 positively recite:

1. A group management system comprising:

09/344,693

a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and

a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes. (Emphasis added)

18. A method for managing a group, the method comprising:  
providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and  
providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes. (Emphasis added)

35. A computer readable medium containing an executable program for managing a group, where the program performs the steps of:  
providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and  
providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes. (Emphasis added)

The Applicants' invention is directed to systems and methods for scalable distributed management of virtual private networks (VPNs). The management of encrypted group communications necessary to establish secure, private VPN communications channels through an underlying public network infrastructure places a variety of burdens on a VPN manager. In particular, the addition or removal of a member from a VPN often involves the generation and distribution of one or more new encryption keys that allow current VPN members to decrypt private communications sent through the VPN, but prevent non-VPN members from decrypting the communications. As VPN membership increases and changes dynamically with greater frequency, the complexity of encryption key management becomes even more burdensome. Thus, the VPN manager becomes a single point of failure for the entire VPN; overload of the VPN manager can cause the entire VPN to fail. This makes the VPN architecture very difficult and very costly to scale, which is not ideal for enterprises

09/844,693

relying on secure and private electronic communications.

The Applicants' invention enhances the scalability of a VPN by dividing the member nodes of the VPN, which communicate with each other via encrypted communications, into subsets and providing a plurality of master nodes that are each associated with a subset of member nodes to control membership (i.e., admission and departure) in the VPN for that subset. For example, each master node is responsible for managing the generation and distribution of encryption keys for only its associated subset(s), so that VPN communication and management burdens are not placed entirely on a single master node. This eliminates the single point of failure, because if one master node fails, any one of a plurality of other master nodes is available to assume the failed node's responsibilities. Thus, a VPN employing such an architecture is more easily scalable than a VPN employing a more conventional architecture, because a plurality of new member nodes may be added or admitted to the VPN through a discrete master node.

In contrast, Bots does not teach or suggest that a VPN unit may control membership in a VPN for a subset of interconnected nodes, where all communications between the interconnected nodes are encrypted. The VPN units of Bots control communications to and from associated end stations, which are not equivalent to member nodes of a VPN. For example, only some of the communications between end stations may be encrypted, but not all communications are necessarily encrypted. Thus, the VPN units can not be considered "master nodes" that control admission and departure in a VPN for member nodes, as suggested by the Examiner. Moreover, even if the VPN units may be considered member nodes of a VPN, they are not controlled by master nodes. Thus, if a new VPN unit is added to the VPN (e.g., for a new company branch), a VPN manager must alert the other VPN units to the presence of the new VPN unit and distribute new encryption keys. Thus, Bots does not resolve the scalability and key management issues that the present invention addresses by providing a plurality of master nodes that control the admission and departure in a VPN of a subset of interconnected member nodes, where all communications between the interconnected nodes are encrypted.

09/344,693

The Examiner submits that Bots does, in fact teach the limitation of all communications between interconnected member nodes being encrypted. The Applicants respectfully disagree with this assertion, however. In particular, the Applicants submit that the portion of Bots that the Examiner cites to support this limitation at most teaches that communications between VPN units are encrypted (see, Bots, column 6, lines 37-52: "When a data packet is sent between source and destination addresses that are both members of the same VPN group, the VPNU will process the data packet from the sending side in such as way as to ensure that it [is] encrypted, authenticated and optionally compressed ... The receiving VPNU will handle the process of decrypting and authenticating the packet before forwarding it toward the destination endstation.", emphasis added). That is, communications sent or received by the member nodes (source and destination nodes), such as communications between the source and its associated VPNU, or between the destination and its associated VPNU, are not encrypted. It is only the communications between the intermediaries (i.e., the VPNUs) that are encrypted.

Bots thus fails to teach or anticipate a system for scalably managing VPNs that controls the admission and departure in a VPN of a subset of interconnected member nodes, where all communications between the interconnected nodes are encrypted, as positively claimed by the Applicants in claims 1, 18 and 35. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claims 2-3, 19-20 and 36-37 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 2-3, 19-20 and 36-37 are not anticipated by the teachings of Bots. Therefore, the Applicants submit that dependent claims 2-3, 19-20 and 36-37 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

## **II. REJECTION OF CLAIMS 4-17, 21-34 and 38-51 UNDER 35 U.S.C. § 103**

Claims 4-17, 21-34 and 38-51 stand rejected as being unpatentable over Bots in

09/844,693

view of the Pandya et al. patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya"). The Applicants respectfully traverse the rejection.

Bots has been discussed above. Pandya teaches a system for managing network resources in a distributed networking environment. The system includes two main software components: a plurality of "agent" components deployed at various network devices, and one or more "control point" components deployed throughout the network. The agents monitor network resources, as well as the network devices with which they are associated, for example to assess the character and quantity of network resources that are required by the network devices. The agents report this information to the control points, which centrally coordinate and control the deployed agents and monitor the status of network resources. In response to monitored network conditions and the data reported by the agents, the control points may alter the behavior of particular agents in order to provide the required network services and resources to the networked devices.

As discussed, Bots fails to disclose or suggest the novel invention of a virtual private network in which a master node controls the admission and departure in a VPN of a subset of interconnected member nodes, where all communications between the interconnected nodes are encrypted, as claimed in Applicants' amended independent claims 1, 18 and 35, from which claims 4-17, 21-34, and 38-51 depend. Pandya does not bridge this gap in the teachings of Bots. Bots in view of Pandya thus fails to teach or make obvious a system for scalably managing VPNs that controls the admission and departure in a VPN of a subset of interconnected member nodes, where all communications between the interconnected nodes are encrypted, as positively claimed by the Applicants in claims 1, 18 and 35. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 4-17, 21-34, and 38-51 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 4-17, 21-34, and 38-51 are not made obvious by the teachings of Bots in view of Pandya. Therefore, the Applicants submit that

09/844,693

dependent claims 4-17, 21-34, and 38-51 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.


### III. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

1/3/06  
Date

  
Kin-Wah Tong, Attorney  
Reg. No. 39,400  
(732) 530-9404

Patterson & Sheridan, LLP  
595 Shrewsbury Avenue  
Shrewsbury, New Jersey 07702

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**